Nach dem dritten Keplerschen Gesetz sind übrigens auch die Umlaufzeiten auf dem Kreis und auf der Ellipse gleich. Dies hat praktische Bedeutung. Wird nämlich vom Raumschiff eine Raumsonde in die elliptische Bahn abgeschossen, während das Raumschiff auf der Kreisbahn bleibt, so kehrt die Sonde wie ein Bumerang nach einem Umlauf zum Schiff zurück.

Unser Anliegen der Betonung der plötzlichen Anwendbarkeit mathematischer Theorien sollte auch im Unterricht beachtet werden. Vor noch nicht langer Zeit waren Bestrebungen im Gange, den Unterricht in den elementargeometrischen Eigenschaften der Kegelschnitte zu reduzieren. Ein Ziel des Mathematikunterrichts muss aber sein, die *Einheit von Mathematik, Physik, Naturwissenschaft* und *Technik* anzustreben, und dies empfiehlt äusserste Vorsicht bei solchen Reduktionen. Denn genau das, was wir heute abbauen wollen, kann morgen eine lebenswichtige Grundlage eines neuen Zweiges der Wissenschaften werden. Dies lehren unsere beiden Aufgaben, welche die Brennpunktseigenschaften der Kegelschnitte ganz wesentlich benutzen.

Die Schweiz zahlt jährlich hohe Summen an die ESRO (European Space Research Organisation) und dokumentiert damit ihr Interesse an der Raumforschung. Dies verpflichtet die Lehrer der höheren Schulstufen, den Blick ihrer Schüler in diese Richtung zu lenken, damit in einigen Jahren auch junge schweizerische Wissenschaftler in der Raumforschung mitreden können. E. STIEFEL, Zürich

Kleine Mitteilungen

Sur les nombres $a^n + 1$

La solution de M. O. REUTTER donnée à mon problème 430 [El. Math. *18*, 89–90 (1963)] m'a suggéré le théorème suivant:

Théorème. *a étant un entier donné >1, il existe une infinité de nombres naturels n tels que $n \mid a^n + 1$.*

Démonstration. Vu le théorème de M. O. REUTTER (voir l. c.), il suffira de démontrer notre théorème pour les entiers impairs $a > 1$. Dans ce cas on a évidemment $2 \mid a^2 + 1$ et les nombres 2 et $a^2 + 1$ sont tous les deux doubles de nombres impairs.

Lemme. *Si a est un nombre impair > 1, m et $a^m + 1$ sont doubles de nombres impairs et $m \mid a^m + 1$, il existe un nombre $m_1 > m$, tel que m_1 et $a^{m_1} + 1$ sont doubles de nombres impairs et que $m_1 \mid a^{m_1} + 1$.*

Démonstration du lemme. Si $m \mid a^m + 1$ et si m et $a^m + 1$ sont doubles de nombres impairs, on a $a^m + 1 = k\,m$, où k est un nombre impair. Il en résulte que $a^m + 1 \mid a^{mk} + 1$, donc

$$a^m + 1 \,\Big|\, a^{a^m+1} + 1$$

et, a étant impair et $a^m + 1$ pair, le nombre

$$a^{a^m+1} + 1$$

est double d'un nombre impair. Pour $m_1 = a^m + 1$ nous aurons donc $m_1 \mid a^{m_1} + 1$, et m_1 et $a^{m_1} + 1$ seront doubles de nombres impairs et, vu que $a > 1$, on aura $m_1 = a^m + 1 > m$. Le lemme se trouve ainsi démontré.

Notre théorème (pour a impairs > 1) résulte tout de suite de notre lemme et de la remarque que pour a impairs on a $2 \mid a^2 + 1$. W. SIERPIŃSKI, Varsovie

A Note on the Order of an Element in a Ring

The following «anwendungsreiche Satz» [1] [1]) is due to H. MINKOWSKI: *The only rational integral matrix that has a positive power equal to the identity matrix and is congruent to the identity matrix modulo some integer greater than two is itself the identity matrix.* In this note we establish the more general

Theorem. *Let R be a ring with an identity. Let a be an element of finite order in the unit group of R, and let n be a positive integer. If there exists a divisor $m > 1$ of n such that*

(i) *either m is odd or m^2 divides n,*

(ii) $b \in R$ *and* $m\,b = 0$ *implies* $b = 0$,

(iii) $b \in m^e R$, $e = 1, 2, \ldots$ *implies* $b = 0$,

then the order of $a + nR$ in the unit group of R/nR is equal to the order of a in the unit group of R.

In other words, if $\delta(0)$ is the least positive integer δ such that $a^\delta = 1$ and $\delta(n)$ is the least positive integer δ such that $a^\delta \equiv 1$ modulo nR, then $\delta(n) = \delta(0)$ provided, of course, some divisor $m > 1$ of n satisfies the three conditions above. That this conclusion may fail without the stated conditions is evidenced by the following examples, (where in each case, $m = n$ is the only possible choice for the divisor).

First, let R be the ring of integers, $a = -1$, and $n = 2$. In this case (ii) and (iii) are satisfied for $m = 2$. But (i) is not satisfied and $\delta(0) = 2$, $\delta(2) = 1$.

Second, let R be the ring $\{\bar{0}, \bar{1}, \ldots, \bar{8}\}$ of integers modulo 9, $a = \bar{2}$, and $n = 3$. For $m = 3$, conditions (i), (iii) but not (ii) are satisfied. Also, $\delta(0) = 6$ but $\delta(3) = 2$ because $\bar{2} \not\equiv \bar{1}$ and $\bar{2}^2 = \bar{1} + 3 \cdot \bar{1} \equiv \bar{1} \pmod{3R}$.

Third, let R be a ring of rational numbers, $a = -1$, and $n = 3$. For $m = 3$, (i) and (ii) are satisfied, but not (iii). Again $\delta(0) = 2$ but $\delta(3) = 1$ since $-1 = 1 + 3\,(-2/3) \equiv 1 \pmod{3\,R}$.

The theorem itself is a consequence of the following

Lemma. *Let R be a ring with an identity. Let a have finite order in the unit group of R and let m be a positive integer satisfying* (ii) *above. If $\delta(m^e)$ is the order of a in the unit group of $R/m^e R$, then $\delta(m^e) < \delta(m^{e+1})$ implies $\delta(m^{e+1}) < \delta(m^{e+2})$, provided $e > 1$ in case m is even.*

Proof. Let $\delta(m^e) < \delta(m^{e+1})$. Since $a^{\delta(m^e)} \equiv 1 \pmod{m^{e+1}R}$ implies $\delta(m^{e+1}) \mid \delta(m^e)$, which is impossible, we have

$$a^{\delta(m^e)} = 1 + m^e\, b$$

with $b \not\equiv 0 \pmod{mR}$. Also, since $m > 1$ and $e > 1$ in case m is even,

$$a^{m\,\delta(m^e)} \equiv 1 + m^{e+1}\, b \pmod{m^{e+2}R}\,.$$

Thus, by (ii), $\delta(m^{e+2}) \nmid m\,\delta(m^e)$. But $\delta(m^{e+1}) \mid m\,\delta(m^e)$. Consequently $\delta(m^{e+2}) \nmid \delta(m^{e+1})$. Finally, since $\delta(m^{e+1}) \mid \delta(m^{e+2})$, it follows that $\delta(m^{e+1}) < \delta(m^{e+2})$.

We now give a proof of the theorem. Thus, let $m > 1$ divide n such that (i), (ii), and (iii) are satisfied. Suppose first that m is odd. Since $\delta(m^e) \mid \delta(0)$ it is clear from the lemma that $\delta(m^e) = \delta(m)$ for $e = 1, 2, \ldots$. That is,

$$a^{\delta(m)} \equiv 1 \pmod{m^e R},\ e = 1, 2, \ldots .$$

Hence, by (iii), $a^{\delta(m)} = 1$ and $\delta(0) \mid \delta(m)$. Therefore, $\delta(m) = \delta(0)$. Similarly, if m is even then by the lemma and (iii), $\delta(m^2) = \delta(0)$. Consequently since $m \mid n$ and, by (i), $m^2 \mid n$ if m is even, $\delta(0) \mid \delta(n)$. Finally, since $\delta(n) \mid \delta(0)$, it follows that $\delta(n) = \delta(0)$.

[1]) Die Ziffern in eckigen Klammern verweisen auf das Literaturverzeichnis, Seite 108.

The theorem itself can be extended. Indeed, let a be an element of an arbitrary ring R. If there exists a term of the sequence $a, a^2, \ldots, a^k, \ldots$ that is equal to a preceding term, then a is said to have finite period. Specifically, if $a^{\gamma(0)+\delta(0)} = a^{\gamma(0)}$, where $\gamma(0) + \delta(0) > \gamma(0) > 0$, is the first such term, then $a^{\gamma(0)}, a^{\gamma(0)+1}, \ldots$ is a periodic sequence of period $\delta(0)$. Moreover, if n is a positive integer, then there is a first term $a^{\gamma(n)+\delta(n)}$ that is congruent to a preceding term $a^{\gamma(n)}$ modulo nR, and the reduced sequence $a^{\gamma(n)}, a^{\gamma(n)+1}, \ldots$ is periodic of period $\delta(n)$. Clearly the period $\delta(n)$ of $a + nR$ in R/nR divides the period $\delta(0)$ of a in R. In fact, we have the following

Corollary. *Let R be a ring. Let a be an element of finite period in R and let n be a positive integer. If there exists a divisor $m > 1$ of n satisfying conditions* (i), (ii), *and* (iii) *above, then the period of $a + nR$ in R/nR is equal to the period of a in R.*

Proof. This result may be demonstrated by a direct extension of the proof of the theorem above. However, by adopting a suggestion to the author from E. C. DADE, the result may also be obtained as follows. First, if a is of finite period in R, then it is clear from the results above that $a^{\gamma+\delta} = a^{\gamma}$ if and only if $\gamma(0) \leqslant \gamma$ and $\delta(0) \mid \delta$. Hence the element $\tilde{1} = a^{\gamma(0)\delta(0)}$ is idempotent and is an identity of the subring $\tilde{R} = \tilde{1}\, R\, \tilde{1}$ in R. Moreover, since $(\tilde{1}\, a\, \tilde{1})^{\delta(0)} = \tilde{1}\, a^{\delta(0)} = \tilde{1}$, the element $\tilde{a} = \tilde{1}\, a\, \tilde{1}$ is a member of the unit group of $\tilde{R}$ with order $\tilde{\delta}(0) \mid \delta(0)$. Furthermore, $a^{\gamma(0)\,\delta(0)+\tilde{\delta}(0)} = \tilde{1}\, a^{\tilde{\delta}(0)} = \tilde{1}\,\tilde{1} = \tilde{1} = a^{\gamma(0)\,\delta(0)}$ implies $\delta(0) \mid \tilde{\delta}(0)$. Therefore $\delta(0) = \tilde{\delta}(0)$. In a similar manner it may be shown that the order of $\tilde{a} + n\tilde{R}$ in the unit group of $\tilde{R}/n\tilde{R}$ is the period of $a + nR$ in R/nR. Consequently, since conditions (i), (ii), and (iii) are valid for the subring $\tilde{R}$ provided they are valid for R, the corollary is now an immediate consequence of the theorem.

D. W. ROBINSON, Brigham Young University
Provo, Utah, USA

REFERENCE

[1] HERMANN MINKOWSKI, Gesammelte Abhandlungen, vol. I (B. G. Teubner, Leipzig, 1911), p. VIII.

Über die n-dimensionalen Axonometrien

1. Unlängst untersuchte G. SZÁSZ[1]) im 3-dimensionalen euklidischen Raum R_3 die Summe und die Quadratsumme der Verkürzungsverhältnisse in der normalen und schiefen Axonometrie. Er bewies, dass die Quadratsumme der Verkürzungsverhältnisse nur im Falle einer normalen Axonometrie gleich 2 ist und im Falle einer schiefen Axonometrie immer grösser als 2. Weiterhin gibt er $\sqrt{6}$ als obere und 2 als untere Schranke für die Summe der Verkürzungsverhältnisse der normalen Axonometrie, und vermutet, dass diese untere Schranke auch im Falle der schiefen Axonometrie gültig sei.

Das Ziel dieses Aufsatzes ist einerseits die Ausdehnung obiger Untersuchungen in den n-dimensionalen euklidischen Raum R_n, und die elementare Berechnung der oberen Schranke der Summe der Verkürzungsverhältnisse der normalen Axonometrie, anderseits die Bestimmung der unteren Schranke der Summe der Verkürzungsverhältnisse der schiefen Axonometrie. Damit wird die SZÁSZsche Vermutung bestätigt.

2. Es ist bekannt, dass im R_3 drei paarweise aufeinander senkrechte Achsen ein Achsenkreuz und seine Projektion auf die Bildebene eine Axonometrie bestimmen.

Steht die Projektionsrichtung senkrecht zur Bildebene, so entsteht eine normale (orthogonale) Axonometrie, im anderen Falle eine schiefe Axonometrie. Das Verhältnis der Bildlänge zur wahren Länge einer auf einer Achse liegenden Strecke ist das Verkürzungsverhältnis bezüglich dieser Achse. Ohne Beschränkung der Allgemeinheit können wir voraussetzen, dass die Bildebene den gemeinsamen Punkt der drei Achsen – den Ursprung des Achsenkreuzes – nicht enthält.

[1]) G. SZÁSZ, *Über die normale Axonometrie*, El. Math. *18*, 58–60 (1963).

Es gibt noch etliche Einschränkungen bezüglich der gegenseitigen Lage von Achsenkreuz, Bildebene und Projektionsrichtung, um die Entartung der Axonometrie zu vermeiden. In den folgenden Untersuchungen werden wir hievon nur eine einzige ausnützen, nämlich dass die Projektionsrichtung zu keiner Koordinatenachse parallel sein darf; mit anderen Worten, jedes Verkürzungsverhältnis muss grösser als null sein.

Analogerweise wird im R_n $(n > 1)$ eine Axonometrie durch die Projektion von n paarweise auf einander senkrechten Achsen (n-dimensionales Achsenkreuz) auf eine $(n-1)$-dimensionale Hyperebene (Bildhyperebene) bestimmt. Wir können ohne Beschränkung der Allgemeinheit voraussetzen, dass die Bildhyperebene den Ursprung nicht enthält. Das Verkürzungsverhältnis bezüglich einer Achse ist das Verhältnis der Projektionslänge auf der Bildhyperebene zur wahren Länge der auf dieser Achse liegenden Strecke.

3. Um die Quadratsumme der Verkürzungsverhältnisse zu bestimmen, folgen wir der Methode von Szász.

Wir bezeichnen mit O den Ursprung des n-dimensionalen $(n \geqq 2)$ Achsenkreuzes, mit A_i $(i = 1, \ldots, n)$ die Schnittpunkte der Koordinatenachsen x_i mit der Bildhyperebene R_{n-1}, und mit S den Spurpunkt des Projektionsstrahles durch O in R_{n-1}. Es sei weiterhin $O A_i = a_i$, und $a'_i = S A_i$ die Projektion auf R_{n-1} $(i = 1, \ldots, n)$, und $O S = t$. Die Gleichung der Bildhyperebene bezüglich des Achsenkreuzes lautet

$$\sum_{i=1}^{n} \frac{\xi_i}{a_i} = 1\,, \tag{1}$$

wo ξ_i $(i = 1, \ldots, n)$ die Koordinaten eines beliebigen Punktes der Bildhyperebene bedeuten. Hat O von R_{n-1} den Abstand d, so gilt bekanntlich die Beziehung

$$\sum_{i=1}^{n} \frac{1}{a_i^2} = \frac{1}{d^2}\,. \tag{2}$$

Geben wir nun dem Spurpunkt S die Koordinaten ξ_i, so wird das Quadrat des Verkürzungsverhältnisses q_i bezüglich der Achse x_i

$$q_i^2 = \frac{a_i'^2}{a_i^2} = \frac{(\xi_i - a_i)^2 + \left(\sum\limits_{i=1}^{n} \xi_i^2\right) - \xi_i^2}{a_i^2} = 1 + \frac{\sum\limits_{i=1}^{n} \xi_i^2}{a_i^2} - 2\,\frac{\xi_i}{a_i}\,.$$

Hieraus folgt

$$\sum_{i=1}^{n} q_i^2 = n + \left(\sum_{i=1}^{n} \xi_i^2\right) \sum_{i=1}^{n} \frac{1}{a_i^2} - 2 \sum_{i=1}^{n} \frac{\xi_i}{a_i}$$

und mit Rücksicht auf (1) und (2)

$$\sum_{i=1}^{n} q_i^2 = n - 2 + \frac{t^2}{d^2}\,.$$

Wegen $t \geqq d$ ist

$$\sum_{i=1}^{n} q_i^2 \geqq n - 1\,. \tag{3}$$

Gleichheit tritt nur dann ein, wenn $t = d$, das heisst, wenn die Projektionsrichtung senkrecht zur Bildhyperebene ist, also im Fall der normalen Axonometrie.

Damit haben wir den folgenden

1. Satz. *Im n-dimensionalen Raum ist die Quadratsumme der Verkürzungsverhältnisse in der normalen Axonometrie – und nur in der normalen Axonometrie – gleich $n - 1$, und in der schiefen Axonometrie immer grösser als $n - 1$.*

Dieser Satz enthält den ersten Satz von Szász, dass im R_3 die Quadratsumme der Verkürzungsverhältnisse genau im Falle der normalen Axonometrie gleich 2 ist, und im Falle der schiefen Axonometrie immer grösser als 2.

4. Es lässt sich leicht einsehen, dass die Summe der Verkürzungsverhältnisse nur im Fall der normalen Axonometrie eine obere Schranke hat.

Wenden wir die bekannte Ungleichung zwischen arithmetischem und quadratischem Mittel

$$\frac{\sum_{i=1}^{n} q_i}{n} \leq \left[\frac{\sum_{i=1}^{n} q_i^2}{n}\right]^{\frac{1}{2}}$$

auf die Verkürzungsverhältnisse an, so ergibt sich mit Rücksicht auf Satz 1

$$\sum_{i=1}^{n} q_i \leq \sqrt{n(n-1)}\,. \tag{4}$$

Es gilt also der folgende

2. Satz. *Im n-dimensionalen Raum ist die Summe der Verkürzungsverhältnisse einer normalen Axonometrie nicht grösser als $\sqrt{n(n-1)}$.*

Dieser Satz enthält den 2. Satz von Szász, der aussagt, dass im R_3 die obere Schranke der Summe der Verkürzungsverhältnisse einer normalen Axonometrie gleich $\sqrt{6}$ ist.

5. Um die untere Schranke der Summe der Verkürzungsverhältnisse einer beliebigen Axonometrie festzustellen, untersuchen wir zuerst die Fälle, in denen keine Koordinatenachse zur Bildhyperebene parallel liegt. Es liegen also sämtliche Schnittpunkte A_i $(i = 1, \ldots, n)$ des Achsenkreuzes mit der Bildhyperebene im Endlichen.

Fall a. Sind sämtliche Verkürzungsverhältnisse kleiner als 1, das heisst $q_i < 1$ $(i = 1, \ldots, n)$, so gilt offenbar $q_i > q_i^2$ also

$$\sum_{i=1}^{n} q_i > \sum_{i=1}^{n} q_i^2$$

und infolge (3)

$$\sum_{i=1}^{n} q_i > n-1\,. \tag{5}$$

Fall b. Es seien nun von den n Verkürzungsverhältnissen q_i die ersten m $(1 < m < n)$ kleiner, und die übrigen $n - m$ grösser oder gleich 1, also

$$\sum_{k=m+1}^{n} q_k \geqq n - m\,.$$

Die Achsen x_j $(j = 1, \ldots, m)$ bilden ein m-dimensionales Achsenkreuz. Wir fassen die durch die Punkte A_j $(j = 1, \ldots, m)$ bestimmte $(m-1)$-dimensionale Hyperebene R_{m-1} als Bildhyperebene auf, und wählen $O\,S'$ als Projektionsrichtung, wo S' die Normalprojektion des Punktes S auf R_{m-1} bezeichnet.

So entsteht eine m-dimensionale Axonometrie mit den Verkürzungsverhältnissen

$$q_j^* = \frac{\overline{S'A_j}}{a_j} \qquad (j = 1, \ldots, m)$$

Aus $\overline{SA_j} \geqq \overline{S'A_j}$ folgt $q_j^* \leqq q_j = \overline{SA_j}/a_j$.

Mittels (5) folgt weiterhin

$$\sum_{j=1}^{m} q_j \geqq \sum_{j=1}^{m} q_j^* > m - 1$$

und damit

$$\sum_{i=1}^{n} q_i = \sum_{j=1}^{m} q_j + \sum_{k=m+1}^{n} q_k > n - 1\,.$$

Wir haben bisher den Fall $m = 1$ bzw. $m = 0$ ausgeschlossen. Für $m = 1$ wird wegen $q_1 > 0$

$$\sum_{i=1}^{n} q_i = q_1 + \sum_{k=2}^{n} q_k \geqq q_1 + n - 1 > n - 1\,.$$

Im Falle $m = 0$ gilt (5) trivialerweise.

6. Liegen nun von den Schnittpunkten A_i $(i = 1, \ldots, n)$ des Achsenkreuzes mit der Bildhyperebene nur m $(1 < m < n)$ im Endlichen, so sind $n - m$ Koordinatenachsen zur Bildhyperebene parallel.

Die Summe der Verkürzungsverhältnisse bezüglich der zur Bildhyperebene nicht parallelen Achsen ist nach Fall b grösser als $m - 1$.

Da jedes Verkürzungsverhältnis auf einer zur Bildhyperebene parallelen Achse gleich 1 ist, ergibt sich

$$\sum_{i=1}^{n} q_i > m - 1 + \sum_{k=m+1}^{n} q_k > n - 1 .$$

Der Fall $m = 0$ schliesst sich von selbst aus, da die Bildhyperebene nicht zu sämtlichen Koordinatenachsen parallel sein kann. Für $m = 1$ wird wegen $q_1 > 0$

$$\sum_{i=1}^{n} q_i = q_1 + n - 1 > n - 1 .$$

Damit haben wir den folgenden Satz bewiesen:

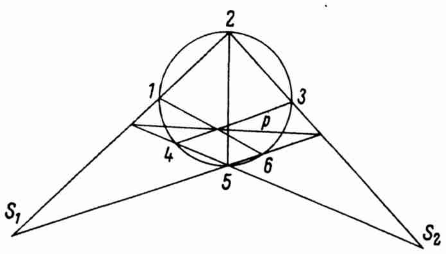
3. Satz. *Im n-dimensionalen Raum ist die Summe der Verkürzungsverhältnisse einer beliebigen Axonometrie immer grösser als $n - 1$.*

Satz 3 enthält für den R_3 die Verschärfung der SzÁsz'schen Behauptung für normale Axonometrie, sowie den Beweis und die Verschärfung seiner Vermutung, dass die Summe der Verkürzungsverhältnisse einer beliebigen Axonometrie im gewöhnlichen Raum nicht kleiner als 2 ist.

J. Schopp, Budapest

Ein Beweis des Pascalschen Satzes

Fig. 1 zeigt die Aussage des Pascalschen Satzes: Wenn die mit 1 bis 6 bezeichneten Punkte auf einem Kegelschnitt – in der Abbildung ein Kreis – liegen, dann liegen die Schnittpunkte 12×45, 23×56, 34×61 auf der Pascalschen Geraden p.



Figur 1

Den Betrachtungen sei ein bekannter Satz vorausgeschickt, der Vollständigkeit halber mit Beweis.

Zwei Flächen 2.O. $[F_1]$, $[F_2]$ sollen den Kegelschnitt (K) gemeinsam haben. Die Ebene dieses Kegelschnittes sei die Ebene $z = 0$ eines x, y, z-Koordinatensystems. Die Gleichungen der beiden Flächen lauten dann nach Potenzen von z geordnet

$$a_1 z^2 + z (b_1 x + c_1 y + d_1) + K (x, y) = 0 , \qquad (1)$$

$$a_2 z^2 + z (b_2 x + c_2 y + d_2) + K (x, y) = 0 , \qquad (2)$$

wobei eine der beiden Gleichungen bereits mit einem passenden Faktor multipliziert ist. Zieht man (2) von (1) ab, so ergibt sich

$$z ((a_1 - a_2) z + (b_1 - b_2) x + (c_1 - c_2) y + d_1 - d_2) = z \cdot e (x, y, z) = 0 ,$$

das heisst die Schnittkurve der beiden Flächen besteht aus dem in der Ebene $z = 0$ gelegenen Kegelschnitt $K = 0$ und einem weiteren in der Ebene $e = 0$ gelegenen Kegelschnitt, der speziell auch mit $K = 0$ zusammenfallen kann.